ISSN: 2424-8460(O)
2251-2608(P)

Original Research Article

Research on taxonomies, security risks and policies of digital currency: Based on the perspective of literature review

Shanshan Wu[1], Yuda Wang[2]

1 China Telecom Group Co., Ltd. Cloud Network Operations Department, Beijing, 100010, China
2 China Reinsurance (Group) Co., Ltd Beijing, 100033, China

Abstract: This paper systematically composes the domestic and international research literature on digital currencies, summarizes the origin and related concepts of digital currencies, and elaborates on the classification of digital currencies. Based on the development status of digital currency in recent years, we have deeply studied the technical principles, key technologies and operating modes of digital currencies, analyzed the risk challenges in terms of cyber security, cryptographic security, data security and personal information protection. Finally, this paper provides an expectation on the future development of digital currencies and proposes suggestions for further research in cross-border payment and cyber security.

Keywords: Digital currency; Central bank digital currencies; Money flower; Cyber security; Monetary policy

1. Introduction

1.1. Definition of digital currency

Digital Currency is a carrier that is based on information technology, relies on network transmission, exists in a non-physical form, can carry value and transfer value, and is essentially a string of digital codes.

1.2. Classification of digital currency

Regarding the classification of digital currencies, the *BIS Quarterly Review* proposes the conceptual model of "Money Flower"[1], which classifies digital currencies from four aspects: issuer (central bank or non-central bank), currency form (digital or physical), accessibility (widespread or restricted), and payment transfer. widespread or restricted) and payment transfer mechanism (centralized or decentralized)[2].

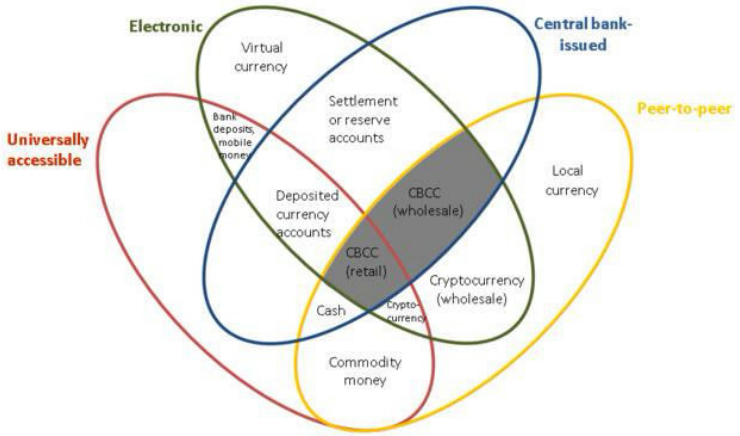

Figure 1. Conceptual model of the "Money Flower".

2. Digital currency development status

Since Satoshi Nakamoto published *Bitcoin: A Peer-to-Peer Electronic Cash System*[3] in 2008, private digital currencies have flourished globally, the types of digital currencies have continued to increase, and the size of the global digital currency market has grown exponentially.Data from the official website of CoinMarketCap shows[4], as of August 10, 2021, the total market capitalization of the global digital currency market is close to $1.85 trillion, and the number of crypto-digital currencies has reached more than 11,206 types.In terms of market share, Bitcoin occupies 46.2% of the market, with Ethereum and Tether taking the second and third places, with 19.8% and 3% of the market, respectively.

3. Digital currency technology principles

3.1. Technical framework

3.1.1. System classification

In terms of system design, digital currency systems can be categorized into two architectural models: Account-Based, or Token-Based.

Account-based means that users will interact strictly with an account representing a long-term relationship, either with a custodian or with the ledger system itself.Token-based means that the token digital currency will exist independently of any particular relationship, just as coins and paper money do.

3.1.2. Token-based

The Token-Based model, where claims are honored only when the user demonstrates knowledge of the cryptographic value (e.g., a digital signature).Transaction parties can trade directly without going through a third party.

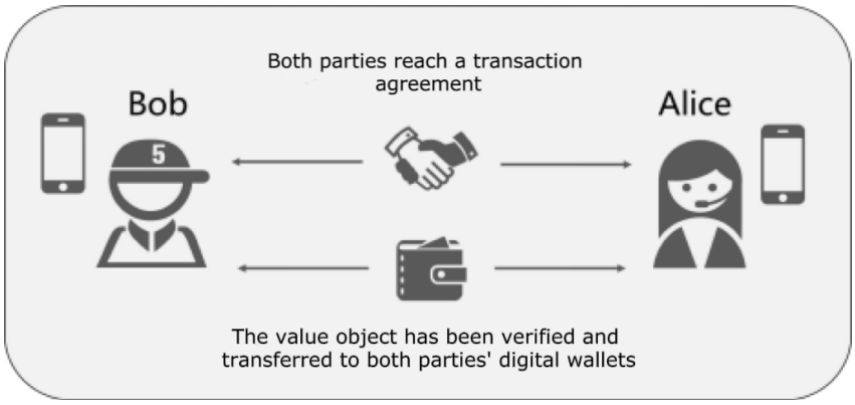

Figure 2. Token-based.

3.1.3. Account-based

In Account-Based model, the ownership of currency is associated with the user's identity, and transactions are authorized through the identity.The Account-Based model requires the involvement of an intermediary institution, such as a central bank or commercial bank.

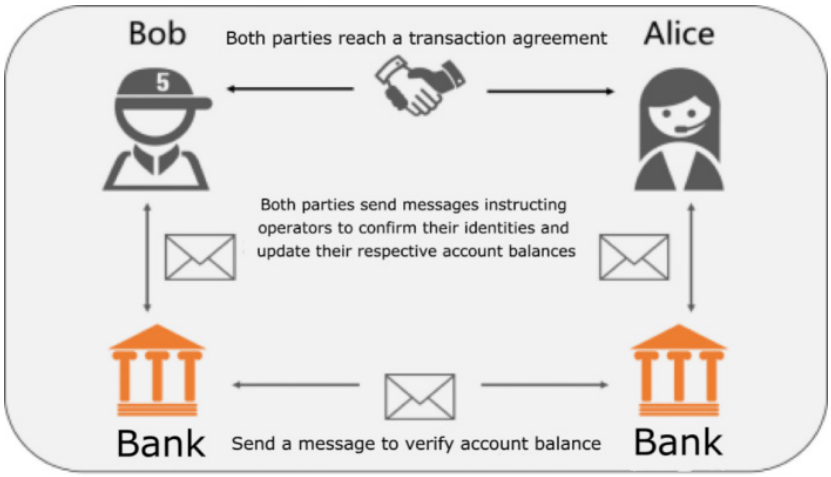

Figure 3. Account-based.

Token-based or account-based is the key to the choice of a central bank digital currency system.The two models correspond to different payment mechanisms, clearing and settlement mechanisms, and very different regulatory mechanisms.Relatively speaking, the token model emphasizes privacy and the account model emphasizes regulation.

3.2. Key technologies

3.2.1. Distributed ledger technology

Distributed Ledger, also known as Shared Ledger, is a consensus for replicating, sharing, and synchronizing digitized data in a network that is geographically distributed across multiple sites, different countries, or institutions[5].Unlike centralized databases, distributed ledgers do not have a central administrator.

Distributed Ledger Technology (DLT), as a broader term, is mostly used to denote a system in which multiple parties participate in the operation of the system in an environment without a central operator or administrator, even if the participants may be unreliable or malicious ("adversarial environment")[6].Blockchain Technology (BT) is often considered to be a particular subset of distributed ledger technology that employs a specific data structure that is composed of blocks of data linked by hashes.

Bitcoin, Ether, Ripple, etc. are typical examples of applications of distributed ledger technology.

3.2.2. Cryptography

Cryptography is the technical science of encoding and decoding, and is the technical practice and study of secure communication in situations where there is a third-party adversary other than the two communicating parties.

Modern cryptography is largely based on mathematical theory and computer science practices; cryptographic algorithms are designed around assumptions of computational difficulty that make them difficult to break in practice by an adversary.

Digital currency is a set of digital simulation of the monetary system, the essence is a string of encrypted data.In the generation and transaction process of digital currency, a large number of cryptographic techniques such as hash function, public key encryption algorithm, zero-knowledge proof, etc. are used to ensure the traceability, non-tampering, non-repudiation and non-falsification of the transaction.

3.2.3. Digital signature

Digital Signature is a method of identifying digital information, mostly based on hash digests and asymmetric key encryption system to realize.The sender of the information produces a set of digital information that cannot be forged by others, and this set of digital information becomes an effective proof of the authenticity of the information sent by the sender.

The use of digital signatures is to verify the integrity and non-repudiation of transaction data, to solve the problem of authentication of digital currency issuers and holders, and to prevent forgery, repudiation, impersonation and tampering.

3.3. Operation system

Take China's digital renminbi (DC/EP) program as an example to illustrate the operation mechanism of the central bank's digital currency.

According to the different responsibilities assumed by the central bank, there are two options for the operation mode of legal tender digital currencies, one is single-tier operation and the other is two-tier operation. The digital RMB adopts a "two-tier operation" model, i.e., the central bank issues the legal tender to a designated operating organization, which is responsible for exchange and circulation transactions.

4. Security risk challenges facing digital currency

4.1. Network security

Central bank digital currencies at the core of the digital currency system are national legal tender based on digital technology. They are not only key information infrastructure in the financial sector but also potential targets for cyber attacks.

Cyber attacks leading to security incidents can cause damage to financial systems, disrupt financial infrastructure, and have a significant impact on financial stability and national security.

4.2. Cryptographic security

Digital currency technology architecture uses cryptographic mechanisms, such as asymmetric encryption, hash algorithms, etc., which are based on the mathematical theory of computational complexity, and are relatively secure for the time being.However, with the rise of artificial intelligence and quantum computing, the research and development of quantum computers with a large number of sub-bits, quantum chips, quantum computing service systems, etc., can crack the large factor decomposition of asymmetric cryptographic algorithms in seconds, which greatly threatens the integrity of the cryptographic algorithms as the underlying security pillars of digital currencies.

4.3. Data security

The current research and piloting of digital currencies by central banks mainly focuses on domestic application scenarios, but central bank digital currencies can also be used for cross-border payments.However, given that most countries and regions have not yet put forward clear regulations and standards for the cross-border use of digital currencies, digital currencies in the cross-border use of certain risks[7].The cross-border transmission, flow and interoperability of financial data between different countries and regions may lead to the transmission of risk linkages between different systems, increasing the complexity of data security management.

4.4. Personal information security

Digital currencies using distributed ledger technology imply that data is shared among all nodes on the network.Some of the network tracking technologies that are currently emerging can ultimately discover the originating node of a transaction by tracking its propagation path through the network.Once a transaction is associated with information such as the IP address of the originating node, it is possible to associate anonymous accounts and user identities in the transaction, thereby destroying the anonymity of the transaction and jeopardizing the security of personal information.

5. Future outlook of digital currency

The current accelerated integration of the real economy and the digital economy, driven by new technologies, the financial market is further digitized, and the era of global digital currency competition is accelerating.

Looking ahead, digital currency theory and practice will continue to innovate, and central bank digital currency will become the mainstream form of digital currency by virtue of its sovereignty advantage.On the other hand, digital currencies will face pressure and challenges from the technical and regulatory levels.As a next step, it is necessary to establish and improve digital currency technical standards, business models and policy frameworks, and actively carry out research and exploration in cross-border payments and other areas; at the same time, it is necessary to thoroughly sort out and assess the risks and challenges faced by digital currencies, strengthen the construction of the network security guarantee system, and guard against and resolve non-traditional security risks in the financial field.

References

[1] Gang Di. Analysis of Digital Currency [J]. China Finance, 2018:52-54.

[2] Morten Linnemann Bech , Rodney Garratt. Central bank cryptocurrencies [J]. BIS Quarterly Review, 2017.

[3] Nakamoto S . Bitcoin: A Peer-to-Peer Electronic Cash System[J]. https://bitcoin.org/bitcoin.pdf.

[4] CoinMarketCap[EB/OL]. https://coinmarketcap.com/zh/coins/views/all/, 2021-08-09.

[5] UK Government Chief Scientific Adviser. Distributed Ledger Technology: Beyond Block Chain[R]. Government Office for Science, 2016.

[6] Rauchs M , Glidden A , Gordon B , et al. Distributed Ledger Technology Systems. A Conceptual Framework[J]. Cambridge Centre for Alternative Finance Reports, 2018.

[7] Bank for International Settlements. Central bank digital currencies for cross-border payments[R/OL] (2021-07-09) [2021-08-17].https://www.bis.org/publ/othp38.pdf